UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/480,231	01/10/2000	JORDAN YAAKOV LEVY	U 013180-1	4087

140 7590 10/07/2003

LADAS & PARRY
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	10

DATE MAILED: 10/07/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/480,231	LEVY, JORDAN YAAKOV	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-15 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 01 January 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-15 have been examined.

Specification

The specification is objected to because the title of the invention is missing at the top of first page of the specification.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-11, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shin et al. U.S. Pat. No. 5987134 (hereinafter Shin) in view of Kingdon U.S. Reissued Pat. No. RE37178 (hereinafter Kingdon), and further in view of Swift et al. U.S. Pat. No. 6377691 (hereinafter Swift).

As per claim 1, Shin discloses a method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp (Shin: Column1 lines10-11: authenticate user's access rights to resources; Column 2 lines 60-67:public key cryptography; Column7 lines 59-63: the user identifying information is made to be a public key pair), the method comprising: the verifier choosing a challenge Q and the verifier sending an initialization message to the prover (Shin: Column 5 lines 12-28: generate access ticket based on the security characteristic information and it serves as the challenge; sends challenging data); the prover sending a commit

message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R) (Shin: Column1 lines 54-67: the procedure of sending commit message; the hardware encrypts the number using the embedded authentication key); the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q (Shin: Column5 lines 12-28: challenge data); the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 21-28: the proving device generates a response by utilizing the access ticket... and return it to the verification device; Column6 lines 18-28: functions of the verification routine) , wherein satisfying the predicate relationship provides an indication that the prover has access to the private key (Shin: Column2 lines 51-55: satisfy a specific predefined relation). The verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 26-28: verify the response); and the verifier determining that the prover has access to the private key based on a result of the performing step (Shin: Column3 lines 3-6: authentication of user's access rights to resources).

Shin does not explicitly teach the method of sending identification message and use of padding string in the challenge. However, Kingdon teaches a method of letting prover send an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp (Kingdon: Column8 lines 26-38: the user must be first identified by the server), and Kingdon teaches the method of using padding string in the challenge (Kingdon: Column5 lines 40-45: the remainder of the message is filled with zeroes). The teachings of Kingdon and the system of Shin use the

challenge-response system to authenticate the access to private information. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kingdon within the system of Shin because the combination of Shin and Kingdon first authenticates the identity of the prover before verifying the access to the private key to filter out forged provers. Also, the use of padding string enhances the security of a challenge by providing more bits to a message and makes it more difficult to decrypt.

Shin-Kingdon does not explicitly teach the method of computing a random number. However, Swift teaches a method of computing a random number by applying a private function to Y (Swift: Column7 lines 45-52: the random number is based on system data obtained from the operating system of the client computer; Y is similar to the data obtained; Shin: Column 8 line39-43: Use of one way hash function). Therefore, it would have been obvious for one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shin, Kingdon, and Swift because the random number generated by the teachings of Swift is more secure due to the rapidly changing and unpredictable system data.

As per claim 2, Shin further teaches a method of subsequent to the prover verifying that Y=Fp(Q,X), using the value Fp(Q,X) instead of the value Y of the verifier sending step in all subsequent operations using Y (Shin: Column15 lines 26 and 33: F(n,e) is passed down to the next computation).

As per claim 3, Shin further teaches a method of performing the steps iteratively a plurality of times, and the verifier determining step includes determining based on a plurality of results each associated with one of the plurality of times that the performing step is performed

(Shin: Column3 lines 16-47: Apply several calculations to generate response, each calculation is based on result of previous calculation).

As per claim 4-7, Shin further teaches the use of one-way hash function as public or private disguising functions (Shin: Column8 lines 40-43). One-way hash function also serves as pre-image function that is similar to disguising function.

As per claim 8 and 9, Shin further teaches a method according to claims 1 and 3 wherein the public disguising function Fp comprises a public key dependent disguising function Fpp dependent, in part, on the public key Kp, and Y is equal to Fpp(Q,X,Kp), and the prover verifying step comprises the prover verifying that Y=Fpp(Q,X,Kp) (Shin: Column59-63: user identifying information is made to be a public key pair and access ticket or challenge is based on public key). It would have been obvious to one having ordinary skill in the art to use disguising function on the public key, access ticket, and padding string instead of access ticket and padding string to raise the level of security of the message.

As per claim 10 and 11, Shin further teaches a method according to claims 1 and 3, and wherein the function comprises R^2 modulo N (Column 10 line 23).

As per claim 14, Shin teaches a system for verifying access to a private key associated with a public key Kp, the system comprising: a verifier; and a prover comprising a disguising unit (Shin: Column1 lines10-11: authenticate user's access rights to resources; Column 2 lines 60-67:public key cryptography; Column7 lines 59-63: the user identifying information is made to be a public key pair; Column8 lines 40-43: one-way hash function also serves as pre-image function that is similar to disguising function), the verifier choosing a challenge Q and the verifier sending an initialization message to the prover (Shin: Column 5 lines 12-28: generate

access ticket based on the security characteristic information and it serves as the challenge; sends challenging data); the prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R) (Shin: Column1 lines 54-67: the procedure of sending commit message; the hardware encrypts the number using the embedded authentication key); the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q (Shin: Column5 lines 12-28: challenge data); the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 21-28: the proving device generates a response by utilizing the access ticket... and return it to the verification device; Column6 lines 18-28: functions of the verification routine) , wherein satisfying the predicate relationship provides an indication that the prover has access to the private key (Shin: Column2 lines 51-55: satisfy a specific predefined relation). The verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 26-28: verify the response); and the verifier determining that the prover has access to the private key based on a result of the performing step (Shin: Column3 lines 3-6: authentication of user's access rights to resources).

Shin does not explicitly teach the method of sending identification message and use of padding string in the challenge. However, Kingdon teaches a method of letting prover send an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp (Kingdon: Column8 lines 26-38: the user must be first identified by the server), and Kingdon teaches the method of using padding string in the challenge (Kingdon: Column5 lines 40-45: the remainder

of the message is filled with zeroes). The teachings of Kingdon and the system of Shin use the challenge-response system to authenticate the access to private information. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kingdon within the system of Shin because the combination of Shin and Kingdon first authenticates the identity of the prover before verifying the access to the private key to filter out forged provers. Also, the use of padding string enhances the security of a challenge by providing more bits to a message and makes it more difficult to decrypt.

Shin-Kingdon does not explicitly teach the method of computing a random number. However, Swift teaches a method of computing a random number by applying a private function to Y (Swift: Column7 lines 45-52: the random number is based on system data obtained from the operating system of the client computer; Y is similar to the data obtained; Shin: Column 8 line39-43: Use of one way hash function). Therefore, it would have been obvious for one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shin, Kingdon, and Swift because the random number generated by the teachings of Swift is more secure due to the rapidly changing and unpredictable system data.

As per claim 15, Shin teaches a prover for use with a verifier for verifying access to a private key associated with a public key Kp, the prover comprising: a disguising unit (Shin: Column1 lines10-11: authenticate user's access rights to resources; Column 2 lines 60-67:public key cryptography; Column7 lines 59-63: the user identifying information is made to be a public key pair; Column8 lines 40-43: one-way hash function also serves as pre-image function that is similar to disguising function), wherein the verifier choosing a challenge Q and the verifier sending an initialization message to the prover (Shin: Column 5 lines 12-28: generate access

ticket based on the security characteristic information and it serves as the challenge; sends challenging data); the prover sending a commit message to the verifier, the commit message comprising a disguised form of R produced by applying a function f to R, the disguised form of R being equal to f(R) (Shin: Column1 lines 54-67: the procedure of sending commit message; the hardware encrypts the number using the embedded authentication key); the verifier sending a challenge message to the prover, the challenge message comprising the challenge Q (Shin: Column5 lines 12-28: challenge data); the prover sending a response message to the verifier, the response message comprising a response A, the response A satisfying a predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 21-28: the proving device generates a response by utilizing the access ticket... and return it to the verification device; Column6 lines 18-28: functions of the verification routine) , wherein satisfying the predicate relationship provides an indication that the prover has access to the private key (Shin: Column2 lines 51-55: satisfy a specific predefined relation). The verifier verifying that A satisfies the predicate relationship Pred(A,Q,f(R),Kp) (Shin: Column5 lines 26-28: verify the response); and the verifier determining that the prover has access to the private key based on a result of the performing step (Shin: Column3 lines 3-6: authentication of user's access rights to resources).

Shin does not explicitly teach the method of sending identification message and use of padding string in the challenge. However, Kingdon teaches a method of letting prover send an identification message to the verifier, the identification message comprising an indication of an identity of the prover, the indication of the identity including an indication of Kp (Kingdon: Column8 lines 26-38: the user must be first identified by the server), and Kingdon teaches the method of using padding string in the challenge (Kingdon: Column5 lines 40-45: the remainder

of the message is filled with zeroes). The teachings of Kingdon and the system of Shin use the challenge-response system to authenticate the access to private information. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kingdon within the system of Shin because the combination of Shin and Kingdon first authenticates the identity of the prover before verifying the access to the private key to filter out forged provers. Also, the use of padding string enhances the security of a challenge by providing more bits to a message and makes it more difficult to decrypt.

Shin-Kingdon does not explicitly teach the method of computing a random number. However, Swift teaches a method of computing a random number by applying a private function to Y (Swift: Column7 lines 45-52: the random number is based on system data obtained from the operating system of the client computer; Y is similar to the data obtained; Shin: Column 8 line39-43: Use of one way hash function). Therefore, it would have been obvious for one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shin, Kingdon, and Swift because the random number generated by the teachings of Swift is more secure due to the rapidly changing and unpredictable system data.

4. Claims 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shin in view of Swift.

As per claim 12, Shin teaches a method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp (Shin: Column1 lines 10-11: authenticate user's access rights to resources; Column 2 lines 60-67:public key cryptography; Column7 lines 59-63: the user identifying information is made to be a public key pair), in which the method comprises the prover generating a random number R and communicating a disguised form of the

random number R to the verifier (Shin: Column1 lines 54-67: the procedure of sending commit message; the hardware encrypts the number using the embedded authentication key). Shin does not explicitly teach the method of prover generating the random number R based on an input received from the verifier. However, Swift teaches the method of generating random number based on an input (Swift: Column7 lines 45-52: the random number is based on system data obtained from the operating system of the client computer).

Therefore, it would have been obvious for one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Swift within the system of Shin because the random number generated by the teachings of Swift is more secure due to the rapidly changing and unpredictable system data.

5. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shin in view of Swift as applied to claim 12 above, and further in view of Chaum U.S. Pat. No.6434238 (hereinafter Chaum).

As per claim 13, Shin-Swift teaches a method of receiving input from verifier as described in claim 12. Shin-Swift does not explicitly teach the input received from the verifier includes a commitment to a future query. However, Chaum teaches the method of prover verifying, upon receipt of the future query, that the future query matches the commitment (Chaum: Column25 lines 14-21: Use commit message to verify the response). Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shin, Swift, and Chaum because including commitment in the input further enhances the security of the system by making sure that two parties have certain understanding about each other instead of simple zero-knowledge proof.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kigo et al. U.S. Pat. No. 6073234 discloses device for authenticating user's access rights to resources.

Aratani et al. U.S. Pat. No. 6516413 discloses apparatus and method for user authentication.

Tanaka U.S. Patent Application Publication No. US2001/0005899 discloses method and system of controlling usage of simulator and recording medium storing program for controlling usage of simulator.

Kakehi et al. U.S. Pat. No.6353888 discloses access rights authentication apparatus.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:00am to 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Shin-Hon Chen

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner
Art Unit 2131

SC